

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

HASHIMOTO, et al. Group Art Unit: Not yet assigned

Application No.: New Examiner: Not yet assigned

Filed: Concurrently Herewith Attorney Dkt. No.: 108391-00038

For: **MEMORY DEVICE, MEMORY ACCESS LIMITING SYSTEM, AND MEMORY ACCESS METHOD**

CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Date: March 24, 2004

Sir:

The benefit of the filing dates of the following prior foreign application(s) in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

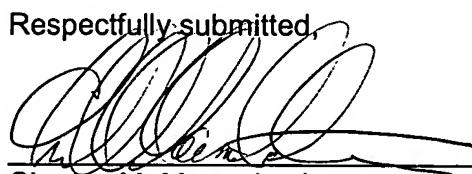
Japanese Patent Application No. 2003-097401 filed on March 31, 2003

In support of this claim, certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of these/this document.

Please charge any fee deficiency or credit any overpayment with respect to this paper to Deposit Account No. 01-2300.

Respectfully submitted,



Charles M. Marmelstein
Registration No. 25,895

Customer No. 004372
AREN'T FOX KINTNER PLOTKIN & KAHN, PLLC
1050 Connecticut Avenue, N.W.,
Suite 400
Washington, D.C. 20036-5339
Tel: (202) 857-6000
Fax: (202) 638-4810
CMM/jch

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application: 2003年 3月31日

出願番号 Application Number: 特願2003-097401

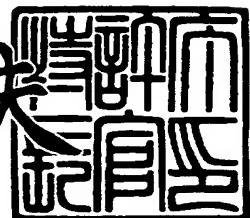
[ST. 10/C]: [JP2003-097401]

出願人 Applicant(s): 富士通株式会社
株式会社エフ・エフ・シー

2003年11月26日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 0251753

【提出日】 平成15年 3月31日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/14

【発明の名称】 メモリ装置、メモリアクセス制限システムおよびメモリ
アクセス方法

【請求項の数】 10

【発明者】

【住所又は居所】 東京都日野市富士町1番地 株式会社エフ・エフ・シー
内

【氏名】 橋本 勝彦

【発明者】

【住所又は居所】 東京都日野市富士町1番地 株式会社エフ・エフ・シー
内

【氏名】 大久保 博

【発明者】

【住所又は居所】 東京都日野市富士町1番地 株式会社エフ・エフ・シー
内

【氏名】 清田 昌紀

【発明者】

【住所又は居所】 東京都日野市富士町1番地 株式会社エフ・エフ・シー
内

【氏名】 三石 俊二

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通
株式会社内

【氏名】 升谷 江一

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【特許出願人】

【識別番号】 000237156

【氏名又は名称】 株式会社エフ・エフ・シー

【代理人】

【識別番号】 100104190

【弁理士】

【氏名又は名称】 酒井 昭徳

【手数料の表示】

【予納台帳番号】 041759

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9906241

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 メモリ装置、メモリアクセス制限システムおよびメモリアクセス方法

【特許請求の範囲】

【請求項 1】 データの読み出しありおよび書き込みが可能で、暗号化されていないデータを記憶する不揮発性の第1のデータ領域と、

データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第2のデータ領域と、

データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第3のデータ領域と、

前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとが一致するときに前記第1のデータ領域に対するデータの読み出しありまたは書き込みをおこなう制御部と、

を具備することを特徴とするメモリ装置。

【請求項 2】 前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとを比較する比較部をさらに具備することを特徴とする請求項1に記載のメモリ装置。

【請求項 3】 前記比較部は、前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとが一致するときに前記第1のデータ領域に対するデータの読み出しありまたは書き込みを許可し、前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとが異なるときに前記第1のデータ領域に対するデータの読み出しありおよび書き込みを禁止することを特徴とする請求項2に記載のメモリ装置。

【請求項 4】 データの読み出しありおよび書き込みが可能で、前記第2のデータ領域に格納されるデータと同じデータを暗号化したデータが格納される不揮発性の第4のデータ領域をさらに具備することを特徴とする請求項1～3のいずれか一つに記載のメモリ装置。

【請求項 5】 データの読み出しありおよび書き込みが可能で、暗号化されていないデータを記憶する不揮発性の第1のデータ領域、データの書き込みが可能で

、かつデータの読み出しが不可能な不揮発性の第2のデータ領域、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第3のデータ領域、並びに前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとが一致するときに前記第1のデータ領域に対するデータの読み出しありは書き込みをおこなう制御部を備えたメモリ装置と、

前記第1のデータ領域および前記第2のデータ領域にデータを書き込む書き込み手段と、

前記書き込み手段と前記メモリ装置との間のデータの授受に供せられる第1のインターフェース手段と、

前記第3のデータ領域にデータを書き込むとともに、前記第1のデータ領域に対するデータの読み出しありは書き込みのアクセスをおこなう読み書き手段と、

前記読み書き手段と前記メモリ装置との間のデータの授受に供せられる第2のインターフェース手段と、

を具備することを特徴とするメモリアクセス制限システム。

【請求項6】 前記メモリ装置は、前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとを比較する比較部をさらに備えていることを特徴とする請求項5に記載のメモリアクセス制限システム。

【請求項7】 前記比較部は、前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとが一致するときに前記第1のデータ領域に対するデータの読み出しありは書き込みを許可し、前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとが異なるときに前記第1のデータ領域に対するデータの読み出しありは書き込みを禁止することを特徴とする請求項6に記載のメモリアクセス制限システム。

【請求項8】 前記メモリ装置は、データの読み出しありは書き込みが可能で、前記第2のデータ領域に格納されるデータと同じデータを暗号化したデータが格納される不揮発性の第4のデータ領域をさらに備えていることを特徴とする請求項5～7のいずれか一つに記載のメモリアクセス制限システム。

【請求項9】 リセット後に、データの読み出しありは書き込みが可能な不揮発性の第1のデータ領域に暗号化されていない所定のデータを書き込むとともに

に、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第2のデータ領域にキーデータを書き込み、前記第1のデータ領域に対するデータの読み出しおよび書き込みが禁止された状態にする第1の工程と、

前記第1のデータ領域に対するデータの読み出しおよび書き込みが禁止された状態のときに、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第3のデータ領域に仮のキーデータを書き込む第2の工程と、

前記仮のキーデータが前記キーデータに一致するときに前記第1のデータ領域に対するデータの読み出しありは書き込みを許可し、一方、前記仮のキーデータが前記キーデータと異なるときに前記第1のデータ領域に対するデータの読み出しおよび書き込みを禁止する第3の工程と、

を含むことを特徴とするメモリアクセス方法。

【請求項10】 前記第2の工程の前に、

データの読み出しおよび書き込みが可能な不揮発性の第4のデータ領域に、前記キーデータを暗号化して書き込む第4の工程と、

前記第4のデータ領域に格納されている暗号データを読み出し、該暗号データを復号化して前記キーデータを取得する第5の工程と、

をさらに有し、

前記暗号データの復号化により得られたキーデータを、前記第2の工程において仮のキーデータとして前記第3のデータ領域に書き込むことを特徴とする請求項9に記載のメモリアクセス方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ICを内蔵したメモリ装置、ICを内蔵したメモリ装置へのアクセス制限システム、およびICを内蔵したメモリ装置へのアクセス方法に関し、特に、ICを内蔵したメモリ装置のメモリに記憶された秘密のデータを秘匿する技術に関する。

【0002】

航空貨物には、送り先などの管理をおこなうために、国際航空運送協会（I A

TA) による IATA コードが記されたタグが取り付けられる。一方、IC を内蔵したメモリカード（以下、IC カードとする）は、持ち運びが容易であるという可搬性と、搬送先でのデータの読み出しや書き込みが容易であるという利便性を兼ね備えている。

【0003】

そこで、タグの代わりとして IC カードを用い、IC カードに、荷主の情報、内容物の情報、発着空港の情報、経由地の情報など、より多くの情報を記憶させ、それらの情報の改ざんを防ぐことによって、現状よりもさらに運航上の安全性や、荷物が送り先に届く確実性を高めることができると考えられる。また、航空貨物の管理に限らず、たとえば個人情報などを記憶した IC カードにおいては、秘密にすべき情報が漏洩したり、改ざんされるのを防ぐ必要がある。

【0004】

【従来の技術】

IC カードに記憶された秘密のデータを盗み見られたり、改ざんされるのを防ぐには、IC カードにデータを暗号化して保存しておくのが有効である。また、IC カードにおいて、内蔵するメモリにパスワードを記憶させておき、このパスワードに一致する外部入力があるときに、メモリへのアクセスを許可する構成としたものが公知である（特許文献 1 参照）。この特許文献 1 に開示された IC カードでは、メモリの良否をテストする場合などに、外部入力がパスワードに一致していなくても、メモリにアクセスすることができる。

【0005】

【特許文献 1】

特開平9-204361号公報

【0006】

【発明が解決しようとする課題】

しかしながら、IC カードを航空貨物のタグ代わりに用いる場合、以下に述べる理由により、データの暗号化は好ましくない。航空貨物は、空港でベルトコンベア等に載せられて自動搬送される。そして、航空貨物がゲートを通過する際に、ゲートに備え付けられたアンテナから IC カードに電力が供給される。その電

力により I C カードが駆動され、電磁誘導方式により I C カードに対してデータの読み出しありまたは書き込みがおこなわれる。

【0007】

つまり、航空貨物がゲートを通過している間に、I C カードのメモリに対して、データを暗号化して書き込む処理や、データを復号化して読み出す処理が完了しなければならない。しかし、データの暗号化および復号化には時間がかかるため、I C カードがゲートを通過するわずか1秒にも満たない時間（ミリ秒オーダー）内に、データの書き込みや読み出しの処理を完了させるのは困難である。

【0008】

本発明は、上記問題点に鑑みてなされたものであって、I C カードにデータを暗号化することなく記憶させ、その記憶データの漏洩や改ざんを防ぐことができるメモリ装置を提供することを目的とする。また、本発明は、I C カードに対する、暗号化していないデータの読み出しや書き替えを制限したメモリアクセス制限システムを提供することを目的とする。さらに、本発明は、I C カードに記憶された、暗号化していないデータの盗み見や改ざんのためのアクセスを禁止したメモリアクセス方法を提供することを目的とする。

【0009】

【課題を解決するための手段】

上記目的を達成するため、本発明は、メモリ装置（I C カード）に、データの読み出しあり書き込みが可能な不揮発性の第1のデータ領域（データ領域）と、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第2のデータ領域（キーデータ領域）と、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第3のデータ領域（キーレジスタ）を設ける。そして、第1のデータ領域（データ領域）に暗号化されていない秘密にすべき所定のデータを書き込むとともに、第2のデータ領域（キーデータ領域）にキーデータを書き込むことによって、第1のデータ領域（データ領域）に対するデータの読み出しあり書き込みが禁止された状態となる。第1のデータ領域（データ領域）に対するデータの読み出しあり書き込みは、第3のデータ領域（キーレジスタ）に正しいキーデータが書き込まれたときに許可され、間違ったキーデータ

が書き込まれたときに禁止される。

【0010】

この発明において、メモリ装置（ＩＣカード）に、データの読み出しおよび書き込みが可能な不揮発性の第4のデータ領域（暗号レジスタ）を設け、この第4のデータ領域（暗号レジスタ）に、キーデータを暗号化して書き込んでおき、メモリ装置（ＩＣカード）を受け取った者が、第4のデータ領域（暗号レジスタ）に格納されている暗号データを読み出して復号化することにより正しいキーデータを取得することができる構成としてもよい。

【0011】

この発明によれば、正しいキーデータが入力されたときに、メモリ装置に格納されている秘密データへのアクセスが許可され、間違ったキーデータが入力されたときに、メモリ装置に格納されている秘密データへのアクセスが禁止される。また、秘密データは、メモリ装置に暗号化されずに記憶される。また、キーデータを読み出すことは不可能である。

【0012】

【発明の実施の形態】

以下に、本発明の実施の形態について図面を参照しつつ詳細に説明する。なお、本実施の形態においては、メモリ装置を構成するＩＣカードを送る側を送り手とし、受け取る側を受け手と表す。

【0013】

（実施の形態1）

図1は、本発明にかかるＩＣカードの構成の一例を示すブロック図であり、図2は、ＩＣカードへのアクセス制限システムの概略構成の一例を示す模式図である。

【0014】

図1および図2において、符号1はＩＣカードである。符号2は、書き込み手段を構成し、ＩＣカード1の送り手側のホストとなるコンピュータである。符号3は、読み書き手段を構成し、ＩＣカード1の受け手側のホストとなるコンピュータである。符号4および5は、それぞれＩＣカード1の送り手側および受け手

側のリーダ／ライタである。リーダ／ライタ4, 5は、ICカード1に対するデータの読み出しありは書き込みをおこなう際のデータの授受に供せられるインターフェース手段であり、それぞれのホストコンピュータ2, 3に接続されている。

【0015】

図2に示すように、ICカード1の送り手は、コンピュータ2を操作し、リーダ／ライタ4を介してICカード1へアクセスして、後述するキーデータの登録、ICカード1のメモリへのデータの書き込み、キーデータの暗号化などの処理をおこなう。一方、ICカード1の受け手は、コンピュータ3を操作し、ICカード1へアクセスして、キーデータの認証、ICカード1のメモリからのデータの読み込み、暗号化されたキーデータの復号化などの処理をおこなう。

【0016】

図1に示すように、ICカード1は、メモリ11、キーデータ領域（第2のデータ領域）12、データ領域（第1のデータ領域）13、キーレジスタ（第3のデータ領域）14、比較部15、キーデータ設定フラグ（第5のデータ領域）16、暗号レジスタ（第4のデータ領域）17、リード／ライト制御部（制御部）18および通信部19を備えている。メモリ11は、読み出しありは書き替えが可能な不揮発性のメモリ、たとえば強誘電性メモリや、読み出しありは書き替えが可能な読み出し専用メモリ、たとえば電気的に一括消去可能なフラッシュメモリや電気的に消去可能なEEPROMなどにより構成される。

【0017】

メモリ11は、キーデータを格納するキーデータ領域12と、送り手または受け手によりデータの書き込みありは読み出しが可能なデータ領域13を備えている。特に限定しないが、たとえばメモリ11は254ブロックで構成されており、そのうちの1ブロックがキーデータ領域12として割り振られ、残りがデータ領域13となる。メモリ11に対するデータの読み出しありは書き込みは、ブロック単位で実施される。

【0018】

キーデータは、データ領域13へのアクセスの許可ありは禁止の設定をおこな

うためのパスワードである。キーデータは、送り手がキーデータ登録処理を実行したときに、リーダ／ライタ4から通信部19を介してリード／ライト制御部18へ送られ、リード／ライト制御部18の書き込み制御によりキーデータ領域12に書き込まれる。キーデータ領域12に対しては、データの書き替えのみをおこなうことができる。つまり、キーデータ領域12にキーデータを書き込むことはできるが、書き込まれたキーデータをキーデータ領域12から読み出すことはできない。

【0019】

キーレジスタ14は、キーデータ領域12に書き込まれたキーデータと比較されるデータを格納する領域である。送り手または受け手がキーデータ認証処理時に入力したデータは、リーダ／ライタ4, 5から通信部19を介してキーレジスタ14に書き込まれる。キーレジスタ14に格納されたデータを読み出すことはできない。キーレジスタ14に対するデータの書き替えのみが可能である。

【0020】

比較部15は、キーデータ領域12に格納されているキーデータと、キーレジスタ14に格納されているデータとの比較をおこなう。比較の結果が一致であれば、メモリ11および暗号レジスタ17に対してイネーブル信号がアサートされ、データ領域13のアクセスおよび暗号レジスタ17のアクセスが許可される。不一致の場合には、イネーブル信号がネゲートされ、データ領域13のアクセス禁止、および暗号レジスタ17に対するライトが禁止される。

【0021】

キーデータ設定フラグ16は、キーデータ領域12に対するキーデータの書き込み処理が実行されたときに、たとえばリード／ライト制御部18の書き込み制御によりセットされる。キーデータ設定フラグ16がセットされているときには、比較部15における2つのデータの比較、および比較結果に基づいたメモリ11に対するイネーブル信号のアサートまたはネゲートが有効となり、上述したように、データ領域13へのアクセスが許可または禁止される。キーデータ設定フラグ16がセットされていない状態、すなわちキーデータ領域12にキーデータが書き込まれていない状態のときには、比較部15から出力されるイネーブル信

号は常にアサートされ、データ領域13へのアクセスは許可される。

【0022】

暗号レジスタ17は、暗号化されたキーデータ（以下、暗号データとする）を格納する領域である。送り手がキーデータの暗号化処理を実行すると、キーデータは、コンピュータ2（図2参照）により暗号化される。その暗号データは、リーダ／ライタ4から通信部19を介して暗号レジスタ17に書き込まれる。暗号レジスタ17に対しては、暗号データの書き込みだけでなく、読み出しもおこなうことができる。受け手は、暗号レジスタ17に格納された暗号データを、通信部19を介してリーダ／ライタ5で読み込み、コンピュータ3（図2参照）により復号化することによって、キーデータ領域12に格納されているキーデータを知ることができる。この際、比較部15は、暗号化レジスタ17への書き込みは、キーデータ領域12と、キーレジスタ14のデータが同じ場合のみおこなわせる。暗号化レジスタ17からの読み出しが、キーデータ領域12とキーレジスタ14のデータが同じでも異なっていても可能にする。

【0023】

リード／ライト制御部18は、キーデータ領域12およびデータ領域13に対するデータの書き込みおよび読み出しの制御をおこなう。通信部19は、リーダ／ライタ4、5との間で、たとえば接触式であれば電気的に、あるいは非接触式であれば電磁誘導方式により、データの授受をおこなう。また、通信部19は、リーダ／ライタ4、5から、ICカード1を駆動するための電力の供給を受ける。

【0024】

つぎに、上述した構成のICカードへのアクセス方法について説明する。図3は、実施の形態1にかかるICカードへのアクセス方法を説明するフローチャートである。また、図4および図5は、そのアクセス方法の実行時のメモリ状態を示す模式図である。また、図6および図7は、ICカードとキーデータの授受形態を示す模式図である。

【0025】

まず、送り手は、ICカード1のリセットをおこなう（ステップS301）。

これによって、キーデータ領域12、データ領域13、キーレジスタ14、キーデータ設定フラグ16および暗号レジスタ17を含む全てのメモリ領域が初期化され、ICカード1の使用が可能な状態となる。

【0026】

ついで、送り手は、データ領域13に所望のデータを書き込む（ステップS302）。このとき、キーデータ領域12にはキーデータが書き込まれていないので、データ領域13は、データの書き込みおよび読み出しが可能な状態となっている。

【0027】

データ領域13へのデータの書き込みが終了したら、キーデータを暗号化してICカード1に記憶させるか否かを選択する（ステップS303）。キーデータを暗号化しない場合には（ステップS303：No）、送り手は、キーデータ領域12にキーデータを書き込む（ステップS304）。このとき、キーデータ設定フラグ16がセットされる。これによって、データ領域13は、データの読み出しおよび書き込みが禁止された状態となる。したがって、今後、データ領域13へアクセスする際には、キーデータの入力が必要となる。

【0028】

そして、送り手は、受け手にICカード1を送るとともに、受け手にキーデータ21を知らせる（ステップS305、図6参照）。なお、受け手に送るキーデータ21を、公知の技術により暗号化しておいてもよい。その場合には、送り手は受け手に、暗号化したキーデータ21を復号化するためのパスワードを、別途知らせる必要がある。

【0029】

一方、キーデータを暗号化する場合には（ステップS303：Yes）、送り手は、たとえば受け手が公開している公開鍵を用いてキーデータの暗号化処理をおこない（ステップS311）、その結果得られた暗号データを暗号レジスタ17に書き込む（ステップS312）。また、キーデータ領域12にキーデータを書き込む（ステップS313）。そして、送り手は、受け手にICカード1を送る。それによって、送り手は、受け手にICカード1とともに暗号データを送る

ことができる（図7参照）。

【0030】

キーデータを暗号化する場合について、ここまでの一ICカード1のキーデータ領域12、データ領域13およびレジスタ14、17の変化の様子が図4（a）および同図（b）に示されている。なお、キーデータを暗号化しない場合には、図4（a）において暗号レジスタ17への暗号データの書き込みがおこなわれないため、図4（b）において暗号レジスタ17は空（意味のあるデータが格納されていない状態）となる。

【0031】

受け手がICカード1を受け取った段階では、データ領域13はデータの読み出しおよび書き込みが禁止された状態となっている（図5（a）参照）。暗号レジスタ17に暗号データが書き込まれている場合には、受け手は、たとえば公開鍵に対する秘密鍵を用いて暗号化を解除（暗号データを復号化）し、キーデータを取得する（ステップS314）。そして、キーレジスタ14に、その復号化されたキーデータを書き込む（ステップS306）。

【0032】

一方、受け手が、ICカード1の他に、キーデータ21を受け取った場合には、キーレジスタ14にそのキーデータ21を書き込む（ステップS306）。その際、キーデータ21が暗号化されている場合には、受け手は、送り手から受け取ったパスワードを用いてキーデータ21を復号化しておく。このときの一ICカード1のキーデータ領域12、データ領域13およびレジスタ14、17の様子が図5（a）に示されている。

【0033】

受け手によりキーレジスタ14にキーデータが書き込まれると、ICカード1は、キーデータ領域12に書き込まれているキーデータと、キーレジスタ14にキーデータとしてセットされたデータとが一致するか否かの判定をおこなう（ステップS307）。一致すれば（ステップS307：Yes）、ICカード1は、受け手がデータ領域13へアクセスするのを許可する。それによって、受け手は、データ領域13からデータを読み込みできる（ステップS308）。また、

受け手は、データ領域13にデータを書き込むこともできる。この状態が図5（b）に示されている。一方、不一致の場合には（ステップS307：No）、ICカード1は、データ領域13へのアクセスを禁止し、受け手がデータ領域13からデータを読み出すのを拒否する（ステップS309）。

【0034】

データ領域13へのアクセスが許可され、データ領域13に対するデータの読み出しまだ書き込みが終了した後、再びデータ領域13をアクセス禁止状態にする場合には、受け手は、キーレジスタ14に、キーデータ領域12に書き込まれているキーデータと異なる任意のデータを書き込む。それによって、データ領域13に対するデータの読み出しおよび書き込みが禁止される。この状態が図5（c）および同図（d）に示されている。

【0035】

上述した実施の形態1によれば、外部からキーデータとして入力されたデータと、あらかじめキーデータ領域12に格納されているキーデータとが一致したときにのみ、ICカード1のメモリ11のデータ領域13に対するアクセスが許可されるので、正しいキーデータを知っている者以外が、データ領域13に記憶された秘密データを盗み見したり、改ざんしたりすることを防ぐことができる。

【0036】

また、実施の形態1によれば、データ領域13に、暗号化していないデータを記憶させることができるので、データの暗号化および復号化の処理が不要となり、データ領域13に対するデータの読み出しおよび書き込みの処理を高速におこなうことができる。したがって、航空貨物に添付されるタグの代わりにICカード1を用いても、ICカード1が移動しながらゲートを通過するわずかな時間に、ICカード1に所望の情報を書き込んだり、読み出したりすることができる。

【0037】

また、実施の形態1によれば、ICカード1のメモリ11のキーデータ領域12に対しては、データの書き込みは可能であるが、読み出しができないので、キーデータ領域12からキーデータが漏洩するのを防ぐことができる。

【0038】

(実施の形態2)

実施の形態2は、実施の形態1と同様の構成のICカードに対するアクセス方法の他の例である。ICカードの構成およびICカードへのアクセス制限システムの構成は実施の形態1と同じであるので、それらについては、実施の形態2の説明においても実施の形態1と同じ符号を用いる。

【0039】

図8は、実施の形態2にかかるICカードへのアクセス方法を説明するフローチャートである。また、図9は、そのアクセス方法の実行時のメモリ状態を示す模式図である。

【0040】

まず、送り手は、ICカード1のリセットをおこない、ICカード1を使用可能な状態とする（ステップS801）。このとき、キーデータ領域12、データ領域13、キーレジスタ14、キーデータ設定フラグ16および暗号レジスタ17を含む全てのメモリ領域が初期化される。

【0041】

ついで、送り手は、キーデータ領域12にキーデータを書き込む（ステップS802、図9（a）参照）。このとき、キーデータ設定フラグ16がセットされる。以後、データ領域13へのアクセスが禁止された状態となる。ついで、送り手は、データ領域13にデータを書き込むために、キーレジスタ14にキーデータを入力する（ステップS803、図9（b）参照）。

【0042】

キーレジスタ14にキーデータが入力されると、ICカード1は、キーデータ領域12に書き込まれているキーデータと、キーレジスタ14にキーデータとしてセットされたデータとが一致するか否かの判定をおこなう（ステップS804）。一致すれば（ステップS804：Yes）、データ領域13へのアクセスが許可されるので、送り手は、データ領域13に所望のデータを書き込む（ステップS805、図9（c）参照）。不一致の場合には（ステップS804：No）、ICカード1は、データ領域13へのアクセスを拒否する（ステップS806）。

【0043】

データ領域13へのデータの書き込みが終了したら、暗号化の有無を判断する（ステップS807）。暗号化をおこなわない場合には（ステップS807：N0）、キーデータ領域12にセットされているキーデータを消去するため、送り手は、キーデータ領域12に、キーデータとは異なる任意のデータを書き込む（ステップS808、図9（c）参照）。これによって、キーレジスタ14に新たにセットされたデータが、キーデータ領域12に書き込まれているキーデータと一致しなくなるので、再びデータ領域13へのアクセスが禁止された状態となる。また、キーデータ領域12に書き込まれているキーデータがわからなくなる。したがって、これ以降は、キーデータを知る者以外がデータ領域13へアクセスすることができなくなる。

【0044】

ステップS807以降は、実施の形態1（図3）のステップS303～ステップS314と同じである。したがって、実施の形態1のステップS303、ステップS304、ステップS305、ステップS306、ステップS307、ステップS308、ステップS309、ステップS310、ステップS311、ステップS312、ステップS313およびステップS314を、それぞれステップS807、ステップS808、ステップS809、ステップS810、ステップS811、ステップS812、ステップS813、ステップS821、ステップS822、ステップS823およびステップS824と読み替えて、ステップS807～ステップS824の説明とする。

【0045】

なお、図9（c）および同図（d）には、キーデータを暗号化する場合のキーデータ領域12、データ領域13および暗号レジスタ17の変化の様子が示されている。しかし、キーデータを暗号化しない場合には、図9（c）において暗号レジスタ17への暗号データの書き込みがおこなわれないので、図9（d）において暗号レジスタ17は空（意味のあるデータが格納されていない状態）となる。

【0046】

上述した実施の形態2によれば、実施の形態1と同様に、データ領域13に記憶された秘密データの漏洩および改ざんを防ぐことができるという効果と、データ領域13に対するデータの読み出しおよび書き込みが高速化されるという効果と、ICカード1からキーデータが漏洩するのを防ぐことができるという効果が得られる。

【0047】

(実施の形態3)

実施の形態3は、実施の形態1と同様の構成のICカードにおいて、データ領域13が複数のサブデータ領域に分割され、そのサブデータ領域ごとにアクセスが制限される場合のアクセス方法の一例である。特に限定しないが、ここでは、図10に示すように、データ領域13がAとBの2つのサブデータ領域（Aサブデータ領域131およびBサブデータ領域132とする）に分割されていると仮定して説明する。

【0048】

実施の形態3では、図10に示すように、ICカードには、Aサブデータ領域131に対応する第1のキーデータ領域121と、Bサブデータ領域132に対応する第2のキーデータ領域122が設けられている。また、キーレジスタ141, 142、図示しないキーデータ設定フラグおよび暗号レジスタ171, 172も2個ずつ設けられている。それ以外のICカードの構成、およびICカードへのアクセス制限システムの構成は実施の形態1と同じであるので、実施の形態3の説明においても実施の形態1と同じ符号を用いる。

【0049】

つぎに、上述した構成のICカードへのアクセス方法について説明する。図11は、実施の形態3にかかるICカードへのアクセス方法を説明するフローチャートである。

【0050】

まず、送り手は、ICカード1のリセットにより、キーデータ領域121, 122、サブデータ領域131, 132、キーレジスタ141, 142、キーデータ設定フラグ16および暗号レジスタ171, 172を含む全てのメモリ領域を

初期化して、 I C カード 1 を使用可能な状態とする（ステップ S 1 1 0 1）。

【0051】

ついで、送り手は、データ領域 1 3 を A サブデータ領域 1 3 1 と B サブデータ領域 1 3 2 に分割する（ステップ S 1 1 0 2）。この場合、たとえば A サブデータ領域 1 3 1 とその先頭アドレス、および B サブデータ領域 1 3 2 とその先頭アドレスの対応関係を示すテーブルが、たとえばメモリ 1 1 の所定の領域に作成される。

【0052】

ついで、送り手は、 A サブデータ領域 1 3 1 および B サブデータ領域 1 3 2 の一方または両方に所望のデータを書き込む（ステップ S 1 1 0 3）。ついで、キーデータを暗号化して I C カード 1 に記憶させるか否かを選択する（ステップ S 1 1 0 4）。キーデータを暗号化しない場合には（ステップ S 1 1 0 4：N o）、送り手は、キーデータ領域 1 2 1, 1 2 2 にキーデータを書き込む（ステップ S 1 1 0 5）。その際、 A サブデータ領域 1 3 1 （または B サブデータ領域 1 3 2 ）のアクセスだけを制限し、 B サブデータ領域 1 3 2 （または A サブデータ領域 1 3 1 ）には自由にアクセスできるようにしたい場合には、 A サブデータ領域 1 3 1 に対応するキーデータ領域 1 2 1 （または B サブデータ領域 1 3 2 に対応するキーデータ領域 1 2 2 ）にだけキーデータを書き込めばよい。

【0053】

A サブデータ領域 1 3 1 および B サブデータ領域 1 3 2 の両方ともアクセスを制限する場合には、両方のキーデータ領域 1 2 1, 1 2 2 にキーデータを書き込めばよい。両方のキーデータ領域 1 2 1, 1 2 2 に書き込むキーデータは、同じであってもよいし、異なっていてもよい。キーデータが異なっていれば、 A サブデータ領域 1 3 1 へのアクセスと B サブデータ領域 1 3 2 へのアクセスを独立して制限することができる。

【0054】

キーデータの書き込みとともに、キーデータ設定フラグ 1 6 がセットされ、以後、キーデータが設定されたサブデータ領域 1 3 1, 1 3 2 へのアクセスが禁止された状態となる。送り手は、受け手に I C カード 1 を送るとともに、受け手に

キーデータとそれに対応するサブデータ領域を知らせる（ステップS1106）

。

【0055】

一方、キーデータを暗号化する場合には（ステップS1104：Y e s）、送り手は、キーデータを暗号化し（ステップS1111）、暗号レジスタ171, 172に書き込む（ステップS1112）。そして、キーデータ領域121, 122にキーデータを書き込む（ステップS1113）。Aサブデータ領域131に対応する暗号データは、Aサブデータ領域131に対応する暗号レジスタ171に書き込まれる。同様に、Bサブデータ領域132に対応する暗号データは、Bサブデータ領域132に対応する暗号レジスタ172に書き込まれる。そして、送り手は、受け手にICカード1を送る。

【0056】

暗号レジスタ171, 172に暗号データが書き込まれている場合には、受け手は、暗号化を解除（暗号データを復号化）してキーデータを取得する（ステップS1114）。そして、キーレジスタ141, 142に、復号化されたキーデータのうちの対応するデータを書き込む（ステップS1107）。一方、受け手が、ICカード1の他に、キーデータを受け取った場合には、キーレジスタ141, 142に、対応するキーデータを書き込む（ステップS1107）。

【0057】

ついで、ICカード1は、キーデータの照合をおこない（ステップS1108）、キーデータが一致した場合（ステップS1108：Y e s）、一致したキーデータに対応するサブデータ領域131, 132へのアクセスを許可する。それによって、受け手は、アクセスが許可されたサブデータ領域131, 132からデータを読み込みできる（ステップS1109）。一方、キーデータが一致しない場合（ステップS1108：N o）、その一致しないキーデータに対応するサブデータ領域131, 132へのアクセスが禁止され、受け手のアクセスが拒否される（ステップS1110）。

【0058】

上述した実施の形態3によれば、複数のサブデータ領域131, 132に対し

て独立してアクセスを制限することができる。また、実施の形態1と同様に、データ領域13に記憶された秘密データの漏洩および改ざんを防ぐことができるという効果と、データ領域13に対するデータの読み出しおよび書き込みが高速化されるという効果と、ICカード1からキーデータが漏洩するのを防ぐことができるという効果が得られる。

【0059】

(実施の形態4)

実施の形態4は、実施の形態3と同様に、実施の形態1と同様の構成のICカードにおいて、データ領域13が複数のサブデータ領域に分割され、そのサブデータ領域ごとにアクセスが制限される場合のアクセス方法の他の例である。実施の形態4が実施の形態3と異なるのは、データ領域13に書き込まれるデータの長さに応じて、個々のサブデータ領域の大きさが設定されることである。

【0060】

つまり、実施の形態3では、個々のサブデータ領域の大きさは固定である。それに対して、実施の形態4では、個々のサブデータ領域の大きさは可変である。また、データ領域13に設けられるサブデータ領域の数も可変であり、データ領域13の空き記憶容量がゼロまたはおおよそゼロになるまで、サブデータ領域の数を増やすことができる。

【0061】

特に限定しないが、ここでは、図12に示すように、データ領域13がAとBとCの3つのサブデータ領域（Aサブデータ領域133、Bサブデータ領域134およびCサブデータ領域135とする）に分割されると仮定して説明する。

【0062】

実施の形態4では、図12に示すように、ICカードには、Aサブデータ領域133に対応する第1のキーデータ領域123、Bサブデータ領域134に対応する第2のキーデータ領域124、およびCサブデータ領域135に対応する第3のキーデータ領域125が設けられている。また、キーレジスタ143, 144, 145、図示しないキーデータ設定フラグおよび暗号レジスタ173, 174, 175も3個ずつ設けられている。

【0063】

ただし、キーデータ領域123, 123, 125、キーレジスタ143, 144, 145、図示しないキーデータ設定フラグおよび暗号レジスタ173, 174, 175は、3個ずつに限らず、データ領域13に設けることのできるサブデータ領域の想定される最大数まで設定可能である。それ以外のICカードの構成、およびICカードへのアクセス制限システムの構成は実施の形態1と同じであるので、実施の形態4の説明においても実施の形態1と同じ符号を用いる。

【0064】

つぎに、上述した構成のICカードへのアクセス方法について説明する。図13は、実施の形態4にかかるICカードへのアクセス方法を説明するフローチャートである。

【0065】

まず、送り手は、ICカード1のリセットにより、キーデータ領域123, 124, 125、サブデータ領域133, 134, 135、キーレジスタ143, 144, 145、キーデータ設定フラグ16および暗号レジスタ173, 174, 175を含む全てのメモリ領域を初期化して、ICカード1を使用可能な状態とする（ステップS1301）。

【0066】

ついで、送り手は、データ領域13に所望のデータを書き込む（ステップS1302）。このとき、あるデータの書き込みが完了するごとに（ステップS1303）、そのデータの格納にデータ領域13のどこまでの領域（ブロック）を使用したかを明示するための終了印を書き込む（ステップS1304）。

【0067】

これを図12に示す例で説明すると、Aサブデータ領域133は、データ領域13の先頭から符号136で示す第1の終了印までの領域である。Bサブデータ領域134は、第1の終了印136のつぎのブロックから符号137で示す第2の終了印までの領域である。Cサブデータ領域135は、第2の終了印137のつぎのブロックから符号138で示す第3の終了印までの領域である。

【0068】

ついで、キーデータを暗号化してICカード1に記憶させるか否かを選択する（ステップS1305）。キーデータを暗号化しない場合には（ステップS1305：No）、ついで、送り手は、キーデータ領域123, 124, 125にそれぞれキーデータを書き込む（ステップS1306）。その際、Aサブデータ領域133、Bサブデータ領域134およびCサブデータ領域135の三つの領域に限らず、実施の形態3と同様に、いずれか一つまたは二つの領域だけに対してアクセスを制限し、残りの領域については自由にアクセスできるようにしてもよい。その場合には、実施の形態3と同様に、アクセスを制限する領域に対してのみ、キーデータ領域123, 124, 125にキーデータを書き込めばよい。

【0069】

キーデータの書き込みとともに、キーデータ設定フラグ16がセットされ、以後、キーデータが設定されたサブデータ領域133, 134, 135へのアクセスが禁止された状態となる。送り手は、受け手にICカード1を送るとともに、受け手にキーデータとそれに対応するサブデータ領域を知らせる（ステップS1307）。

【0070】

一方、キーデータを暗号化する場合には（ステップS1305：Yes）、送り手は、キーデータを暗号化し（ステップS1313）、暗号レジスタ173, 174, 175にそれぞれのサブデータ領域133, 134, 135に対応する暗号データを書き込む（ステップS1314）。送り手は、キーデータ領域123, 124, 125にそれぞれキーデータを書き込む（ステップS1315）。そして、送り手は、受け手にICカード1を送る。

【0071】

暗号レジスタ173, 174, 175に暗号データが書き込まれている場合には、受け手は、暗号化を解除（暗号データを復号化）してキーデータを取得する（ステップS1316）。そして、キーレジスタ143, 144, 145に、復号化されたキーデータのうちの対応するデータを書き込む（ステップS1308）。一方、受け手が、ICカード1の他に、キーデータを受け取った場合には、キーレジスタ143, 144, 145に、対応するキーデータを書き込む（ステ

ップS1308)。

【0072】

ついで、ICカード1は、キーデータの照合をおこない(ステップS1309)、キーデータが一致した場合(ステップS1309:Yes)、一致したキーデータに対応するサブデータ領域133,134,135へのアクセスを許可する。受け手が、アクセスが許可されたサブデータ領域133,134,135のいずれかにアクセスすると、ICカード1は、そのアクセスされたサブデータ領域133,134,135を検索して求める。具体的には、ICカード1は、そのアクセスされたサブデータ領域133,134,135の終了印と、その一つ前の終了印を見つけ、その間の領域のデータにアクセスする(ステップS1310)。

【0073】

これを図12に示す例を用いて、たとえばBサブデータ領域134へのアクセスが許可され、受け手がBサブデータ領域134へアクセスする場合について説明する。ICカード1は、Bサブデータ領域134の終了印である第2の終了印137と、その一つ前のAサブデータ領域133の終了印である第1の終了印136を見つける。そして、ICカード1は、第1の終了印136のつぎのブロックから第2の終了印137を含むブロックまでの領域にアクセスする。

【0074】

このようにして、受け手は、アクセスが許可されたサブデータ領域133,134,135からデータを読み込みできる(ステップS1311)。一方、キーデータが一致しない場合(ステップS1309:No)、その一致しないキーデータに対応するサブデータ領域133,134,135へのアクセスが禁止され。受け手のアクセスが拒否される(ステップS1312)。

【0075】

なお、各サブデータ領域133,134,135の末尾に終了印136,137,138を書き込み、終了印136,137,138を目印にしてICカード1がサブデータ領域133,134,135にアクセスする代わりに、各サブデータ領域133,134,135とそのアドレスとの対応関係を示すテーブルを

、たとえばメモリ11の所定の領域に作成し、このテーブルに基づいてサブデータ領域133, 134, 135にアクセスする構成としてもよい。

【0076】

上述した実施の形態4によれば、複数のサブデータ領域133, 134, 135に対して独立してアクセスを制限することができる。また、実施の形態1と同様に、データ領域13に記憶された秘密データの漏洩および改ざんを防ぐことができるという効果と、データ領域13に対するデータの読み出しおよび書き込みが高速化されるという効果と、ICカード1からキーデータが漏洩するのを防ぐことができるという効果が得られる。

【0077】

(付記1) データの読み出しおよび書き込みが可能で、暗号化されていないデータを記憶する不揮発性の第1のデータ領域と、

データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第2のデータ領域と、

データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第3のデータ領域と、

前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとが一致するときに前記第1のデータ領域に対するデータの読み出しあたは書き込みをおこなう制御部と、

を具備することを特徴とするメモリ装置。

【0078】

(付記2) 前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとを比較する比較部をさらに具備することを特徴とする付記1に記載のメモリ装置。

【0079】

(付記3) 前記比較部は、前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとが一致するときに前記第1のデータ領域に対するデータの読み出しあたは書き込みを許可し、前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとが異なるときに前記第

1のデータ領域に対するデータの読み出しおよび書き込みを禁止することを特徴とする付記2に記載のメモリ装置。

【0080】

(付記4) データの読み出しおよび書き込みが可能で、前記第2のデータ領域に格納されるデータと同じデータを暗号化したデータが格納される不揮発性の第4のデータ領域をさらに具備することを特徴とする付記1～3のいずれか一つに記載のメモリ装置。

【0081】

(付記5) 前記比較部は、前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータが一致するときに前記第4のデータ領域に対する暗号化したデータの読み出しありは書き込みを許可し、前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとが異なるときに前記第4のデータ領域に対する暗号化したデータの読み出しのみを許可し、書き込みは禁止することを特徴とする付記4に記載のメモリ装置。

【0082】

(付記6) 前記第2のデータ領域にデータが格納されたときにセットされ、リセット時にクリアされる第5のデータ領域をさらに具備することを特徴とする付記1～5のいずれか一つに記載のメモリ装置。

【0083】

(付記7) 前記第1のデータ領域に書き込まれるデータ、前記第2のデータ領域に書き込まれるデータ、および前記第3のデータ領域に書き込まれるデータが外部から入力されるとともに、前記第1のデータ領域から読み出されたデータを外部へ出力する通信部をさらに具備することを特徴とする付記1～6のいずれか一つに記載のメモリ装置。

【0084】

(付記8) 前記通信部を介して外部から供給される電力により駆動されることを特徴とする付記1～7のいずれか一つに記載のメモリ装置。

【0085】

(付記9) 前記第1のデータ領域は、複数のサブデータ領域に分割され、また前

記制御部は、前記第2のデータ領域にサブデータ領域ごとに格納されたデータと前記第3のデータ領域にサブデータ領域ごとに格納されたデータとが一致するときに、前記サブデータ領域ごとにデータの読み出しありは書き込みをおこなうことと特徴とする付記1～8のいずれか一つに記載のメモリ装置。

【0086】

(付記10) 前記第1のデータ領域および前記第2のデータ領域は、強誘電体の残留分極によってデータを保持する強誘電性メモリにより構成されていることを特徴とする付記1～9のいずれか一つに記載のメモリ装置。

【0087】

(付記11) データの読み出しありは書き込みが可能で、暗号化されていないデータを記憶する不揮発性の第1のデータ領域、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第2のデータ領域、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第3のデータ領域、並びに前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとが一致するときに前記第1のデータ領域に対するデータの読み出しありは書き込みをおこなう制御部を備えたメモリ装置と、

前記第1のデータ領域および前記第2のデータ領域にデータを書き込む書き込み手段と、

前記書き込み手段と前記メモリ装置との間のデータの授受に供せられる第1のインターフェース手段と、

前記第3のデータ領域にデータを書き込むとともに、前記第1のデータ領域に対するデータの読み出しありは書き込みのアクセスをおこなう読み書き手段と、

前記読み書き手段と前記メモリ装置との間のデータの授受に供せられる第2のインターフェース手段と、

を具備することを特徴とするメモリアクセス制限システム。

【0088】

(付記12) 前記メモリ装置は、前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとを比較する比較部をさらに備えていることを特徴とする付記11に記載のメモリアクセス制限システム。

【0089】

(付記13) 前記比較部は、前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとが一致するときに前記第1のデータ領域に対するデータの読み出しありは書き込みを許可し、前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとが異なるときに前記第1のデータ領域に対するデータの読み出しありは書き込みを禁止することを特徴とする付記12に記載のメモリアクセス制限システム。

【0090】

(付記14) 前記メモリ装置は、データの読み出しありは書き込みが可能で、前記第2のデータ領域に格納されるデータと同じデータを暗号化したデータが格納される不揮発性の第4のデータ領域をさらに備えていることを特徴とする付記10～13のいずれか一つに記載のメモリアクセス制限システム。

【0091】

(付記15) 前記比較部は、前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとが一致するときに前記第4のデータ領域に対する暗号化したデータの読み出しありは書き込みを許可し、前記第2のデータ領域に格納されたデータと前記第3のデータ領域に格納されたデータとが異なるときに前記第4のデータ領域に対する暗号化したデータの読み出しありのみを許可し、書き込みは禁止することを特徴とする付記14に記載のメモリアクセス制限システム。

【0092】

(付記16) 前記メモリ装置は、前記第2のデータ領域にデータが格納されたときにセットされ、リセット時にクリアされる第5のデータ領域をさらに備えていることを特徴とする付記10～15のいずれか一つに記載のメモリアクセス制限システム。

【0093】

(付記17) 前記メモリ装置は、前記第1のデータ領域に書き込まれるデータ、前記第2のデータ領域に書き込まれるデータ、および前記第3のデータ領域に書き込まれるデータが前記第1のインターフェース手段を介して前記書き込み手段

から入力されるとともに、前記第1のデータ領域から読み出されたデータを第2のインターフェース手段を介して前記読み書き手段へ出力する通信部をさらに具備することを特徴とする付記10～16のいずれか一つに記載のメモリアクセス制限システム。

【0094】

(付記18) 前記メモリ装置は、前記通信部を介して前記第1のインターフェース手段または前記第2のインターフェース手段から供給される電力により駆動されることを特徴とする付記10～17のいずれか一つに記載のメモリアクセス制限システム。

【0095】

(付記19) 前記第1のデータ領域は、複数のサブデータ領域に分割され、また前記制御部は、前記第2のデータ領域にサブデータ領域ごとに格納されたデータと前記第3のデータ領域にサブデータ領域ごとに格納されたデータとが一致するときに、前記サブデータ領域ごとにデータの読み出しあり書き込みをおこなうことを特徴とする付記10～18のいずれか一つに記載のメモリアクセス制限システム。

【0096】

(付記20) 前記第1のデータ領域および前記第2のデータ領域は、強誘電体の残留分極によってデータを保持する強誘電性メモリにより構成されていることを特徴とする付記10～19のいずれか一つに記載のメモリアクセス制限システム。

【0097】

(付記21) リセット後に、データの読み出しあり書き込みが可能な不揮発性の第1のデータ領域に暗号化されていない所定のデータを書き込むとともに、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性の第2のデータ領域にキーデータを書き込み、前記第1のデータ領域に対するデータの読み出しあり書き込みが禁止された状態にする第1の工程と、

前記第1のデータ領域に対するデータの読み出しあり書き込みが禁止された状態のときに、データの書き込みが可能で、かつデータの読み出しが不可能な不

揮発性の第3のデータ領域に仮のキーデータを書き込む第2の工程と、

前記仮のキーデータが前記キーデータに一致するときに前記第1のデータ領域に対するデータの読み出しありは書き込みを許可し、一方、前記仮のキーデータが前記キーデータと異なるときに前記第1のデータ領域に対するデータの読み出しありは書き込みを禁止する第3の工程と、

を含むことを特徴とするメモリアクセス方法。

【0098】

(付記22) 前記第2の工程の前に、

データの読み出しありは書き込みが可能な不揮発性の第4のデータ領域に、前記キーデータを暗号化して書き込む第4の工程と、

前記第4のデータ領域に格納されている暗号データを読み出し、該暗号データを復号化して前記キーデータを取得する第5の工程と、

をさらに有し、

前記暗号データの復号化により得られたキーデータを、前記第2の工程において仮のキーデータとして前記第3のデータ領域に書き込むことを特徴とする付記21に記載のメモリアクセス方法。

【0099】

以上において本発明は、上述した各実施の形態に限らず、種々変更可能である。また、本発明にかかるメモリ装置は、荷札としてのICカードに限らず、クレジットカードや、身分証明用のICカードや、社員証や従業員証などのICカードにも適用可能である。また、本発明にかかるシステムは、航空貨物における運搬サービスに限らず、宅配等の集荷サービスや、倉庫における保管物の管理サービスなどにも適用可能である。

【0100】

【発明の効果】

本発明によれば、キーデータを読み出すことができず、かつ正しいキーデータが入力されたときに、メモリ装置に格納されている秘密データへのアクセスが許可され、間違ったキーデータが入力されたときに、メモリ装置に格納されている秘密データへのアクセスが禁止されるので、メモリ装置にデータを暗号化するこ

となく記憶させることができ、またその記憶データの漏洩や改ざんを防ぐことができるという効果を奏する。

【図面の簡単な説明】

【図 1】

実施の形態 1 にかかる IC カードの構成を示すブロック図である。

【図 2】

実施の形態 1 にかかる IC カードへのアクセス制限システムの概略構成を示す模式図である。

【図 3】

実施の形態 1 にかかる IC カードへのアクセス方法を説明するフローチャートである。

【図 4】

実施の形態 1 にかかる IC カードの初期化時のメモリ状態を示す模式図である。

【図 5】

実施の形態 1 にかかる IC カードのメモリアクセス時のメモリ状態を示す模式図である。

【図 6】

実施の形態 1 にかかる IC カードにおけるキーデータの授受形態の一例を示す模式図である。

【図 7】

実施の形態 1 にかかる IC カードにおけるキーデータの授受形態の他の例を示す模式図である。

【図 8】

実施の形態 2 にかかる IC カードへのアクセス方法を説明するフローチャートである。

【図 9】

実施の形態 2 にかかる IC カードの初期化時のメモリ状態を示す模式図である。

【図10】

実施の形態3にかかるICカードのメモリマップを示す模式図である。

【図11】

実施の形態3にかかるICカードへのアクセス方法を説明するフローチャートである。

【図12】

実施の形態4にかかるICカードのメモリマップを示す模式図である。

【図13】

実施の形態4にかかるICカードへのアクセス方法を説明するフローチャートである。

【符号の説明】

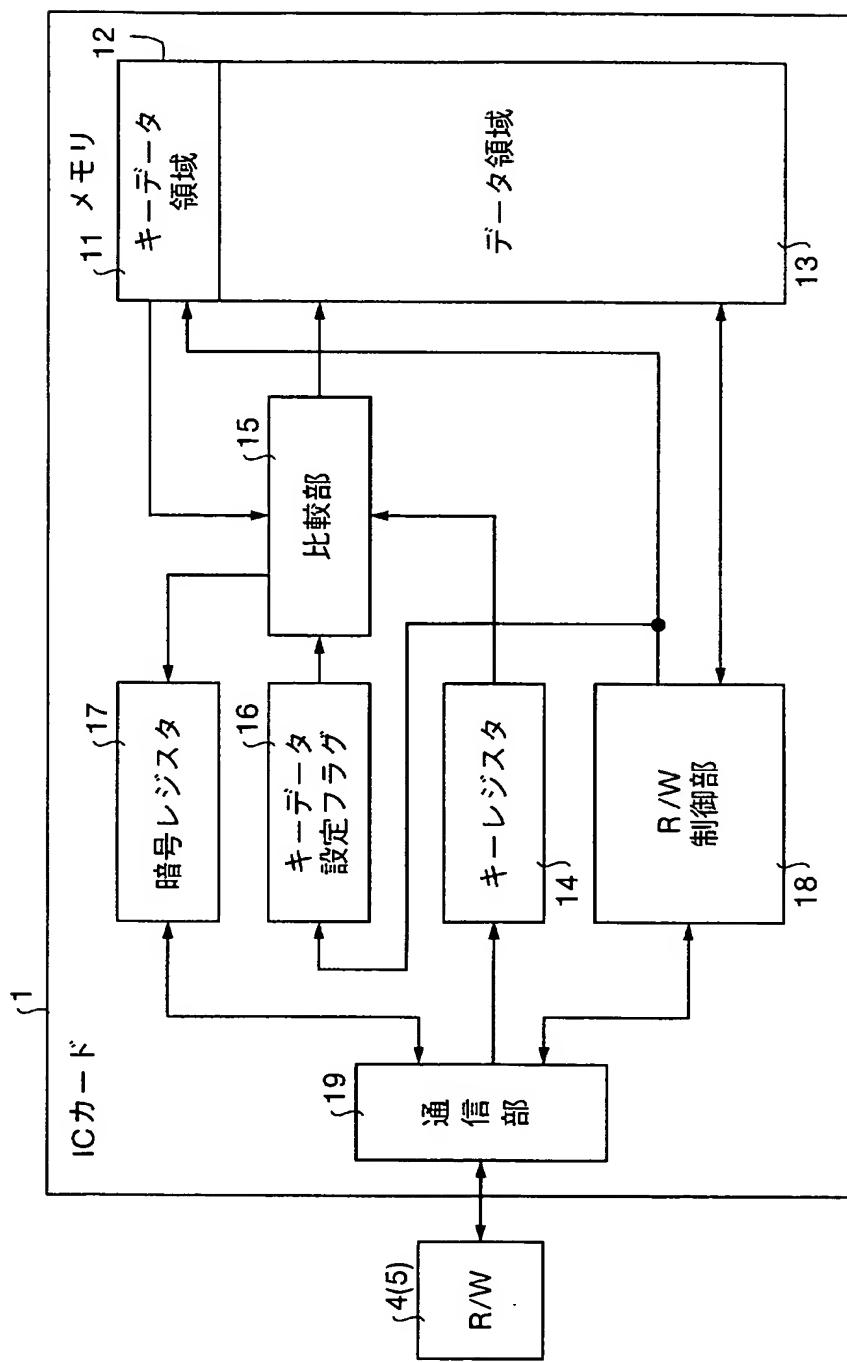
- 1 メモリ装置 (ICカード)
- 2 書き込み手段 (コンピュータ)
- 3 読み書き手段 (コンピュータ)
- 4 第1のインターフェース手段 (リーダ/ライタ)
- 5 第2のインターフェース手段 (リーダ/ライタ)
- 12, 121~125 第2のデータ領域 (キーデータ領域)
- 13 第1のデータ領域 (データ領域)
- 131~135 サブデータ領域
- 14, 141~145 第3のデータ領域 (キーレジスタ)
- 15 比較部
- 16 第5のデータ領域 (キーデータ設定フラグ)
- 17, 171~175 第4のデータ領域 (暗号レジスタ)
- 18 制御部 (リード/ライト制御部)
- 19 通信部

【書類名】

図面

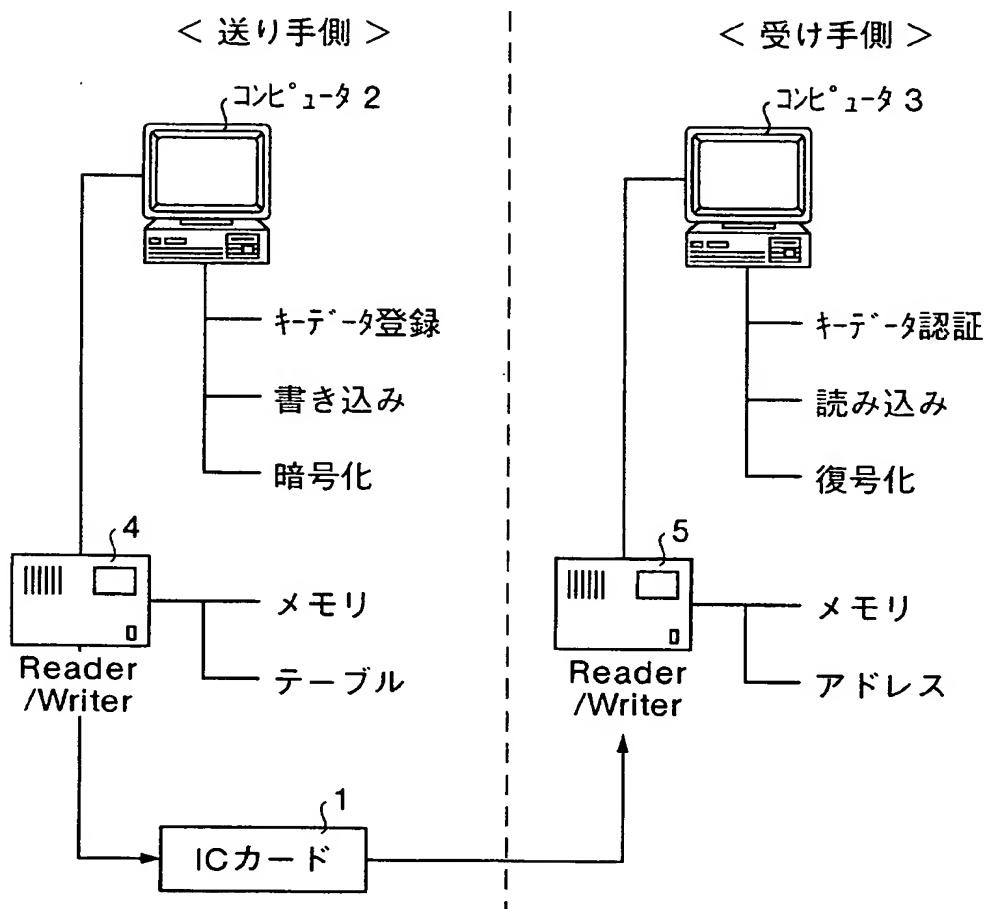
【図 1】

実施の形態1にかかるICカードの構成を示すブロック図



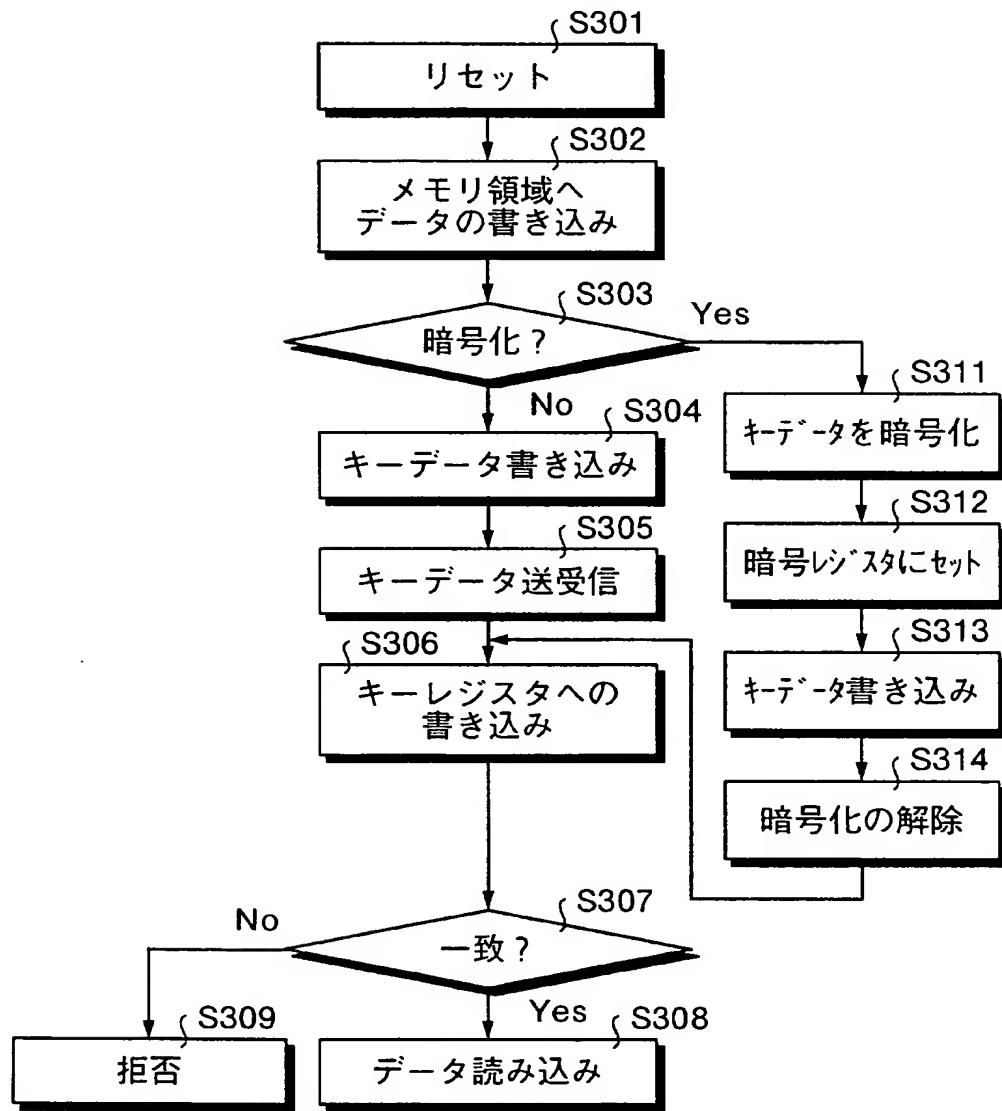
【図2】

実施の形態1にかかる
ICカードへのアクセス制限システムの概略構成を示す模式図



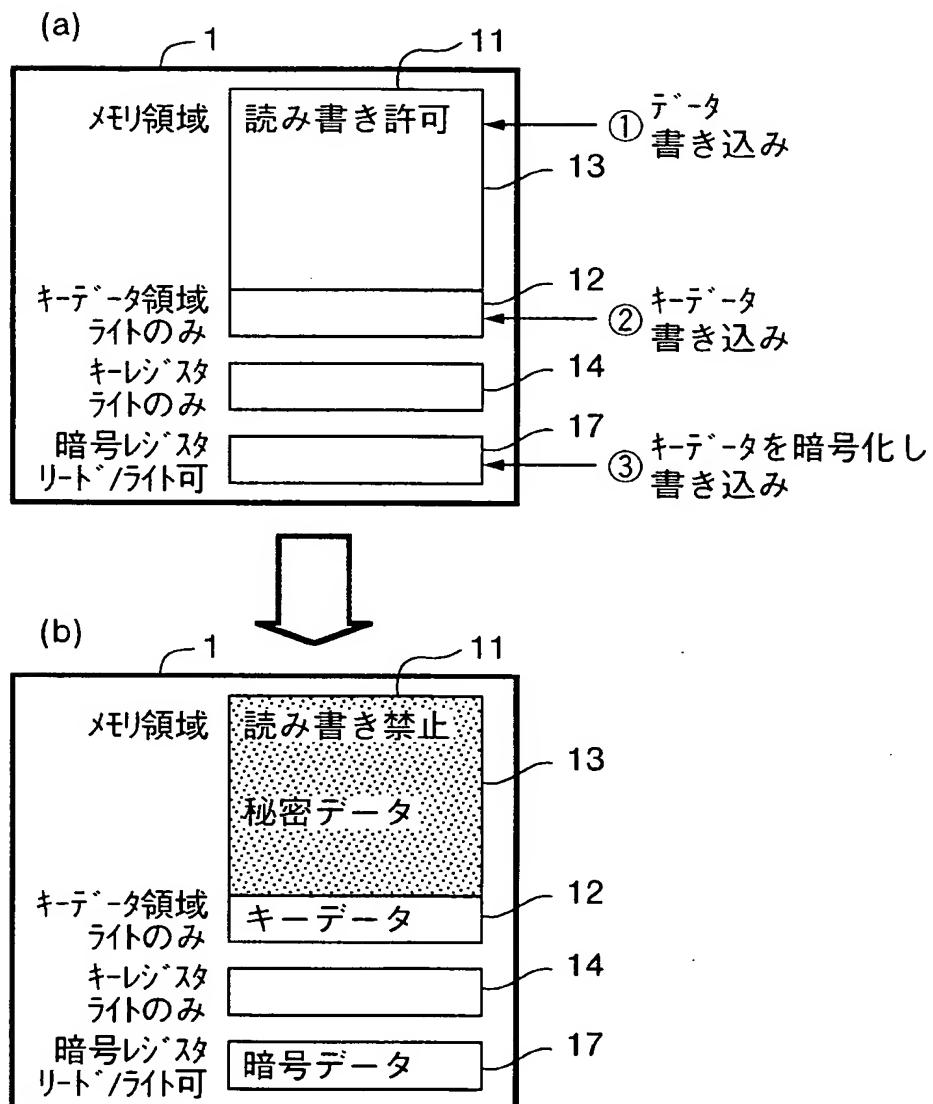
【図3】

実施の形態1にかかる
ICカードへのアクセス方法を説明するフローチャート



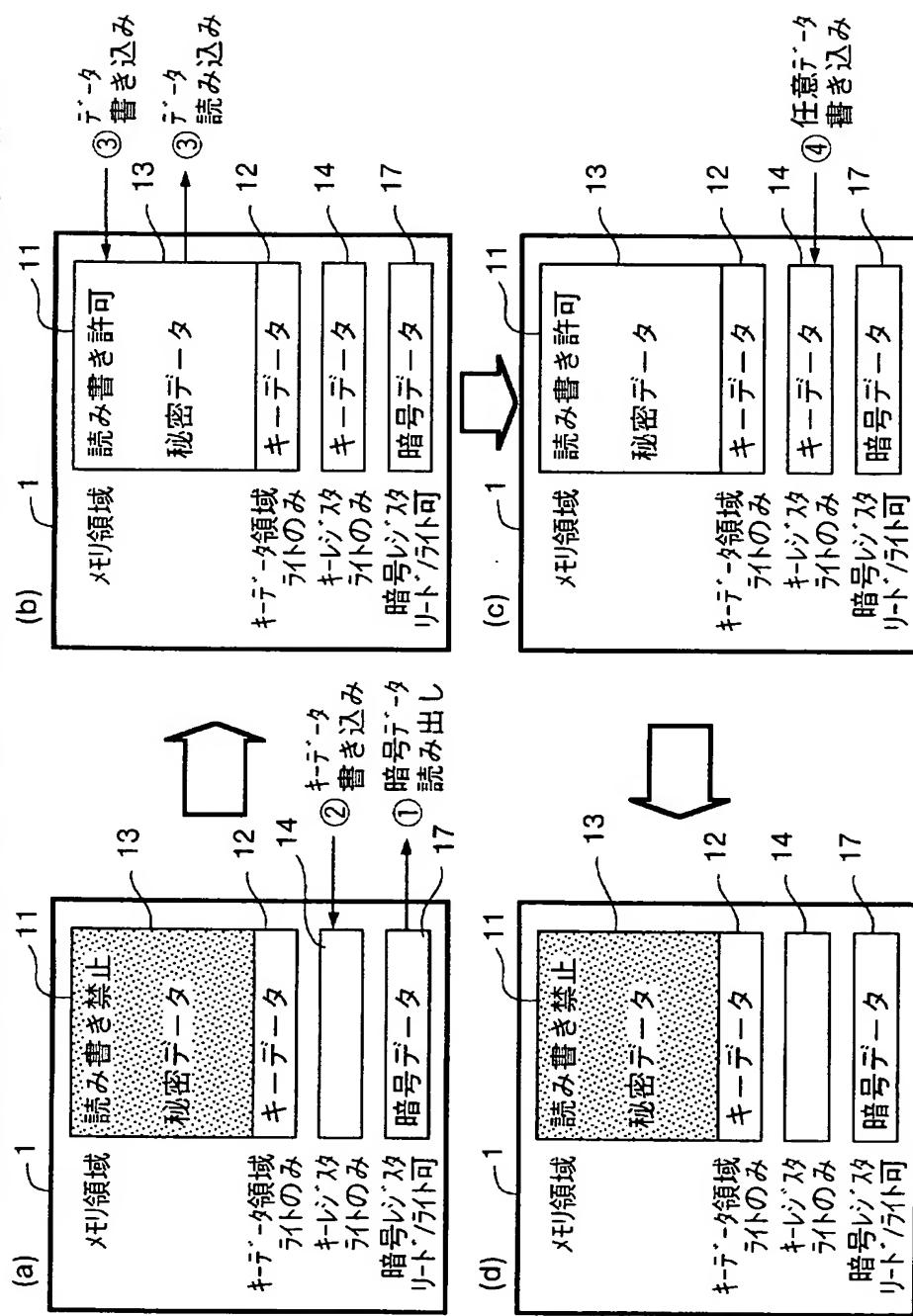
【図 4】

実施の形態 1 にかかる
IC カードの初期化時のメモリ状態を示す模式図



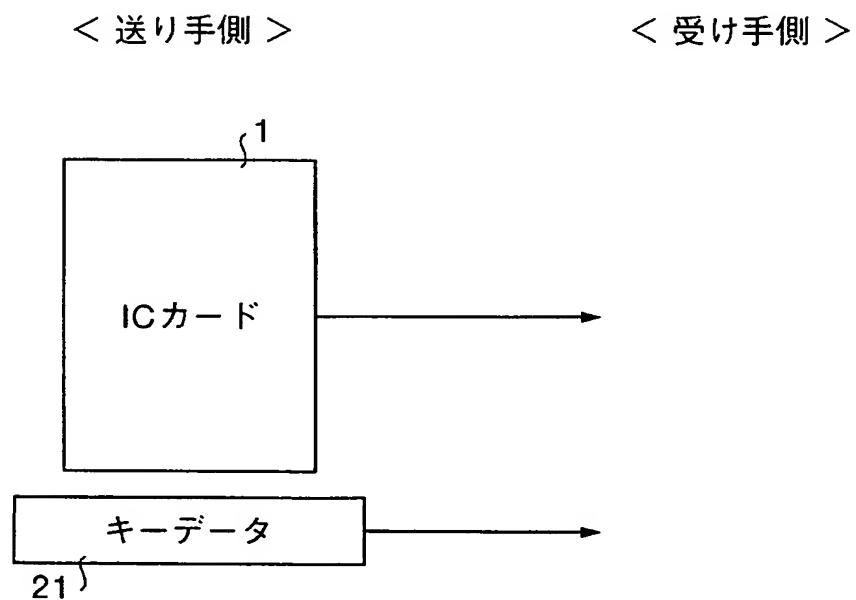
【図5】

本発明の実施の形態1にかかるICカードのメモリアクセス時のメモリ状態を示す模式図



【図6】

実施の形態1にかかる
ICカードにおけるキーデータの授受形態の一例を示す模式図

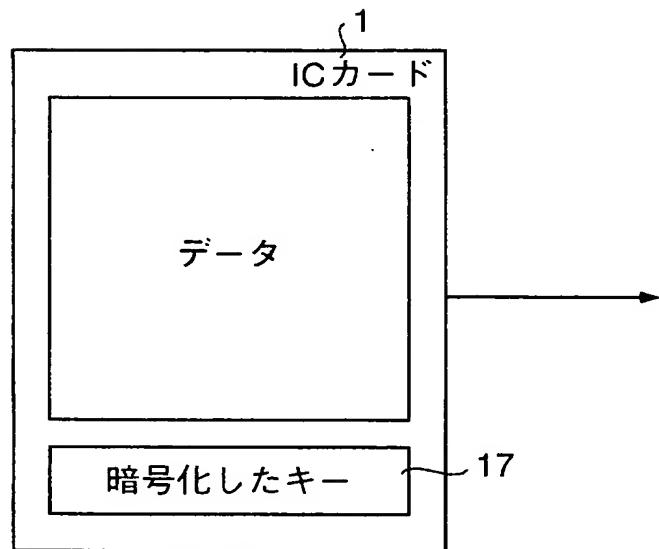


【図7】

実施の形態1にかかる
ICカードにおけるキーデータの授受形態の他の例を示す模式図

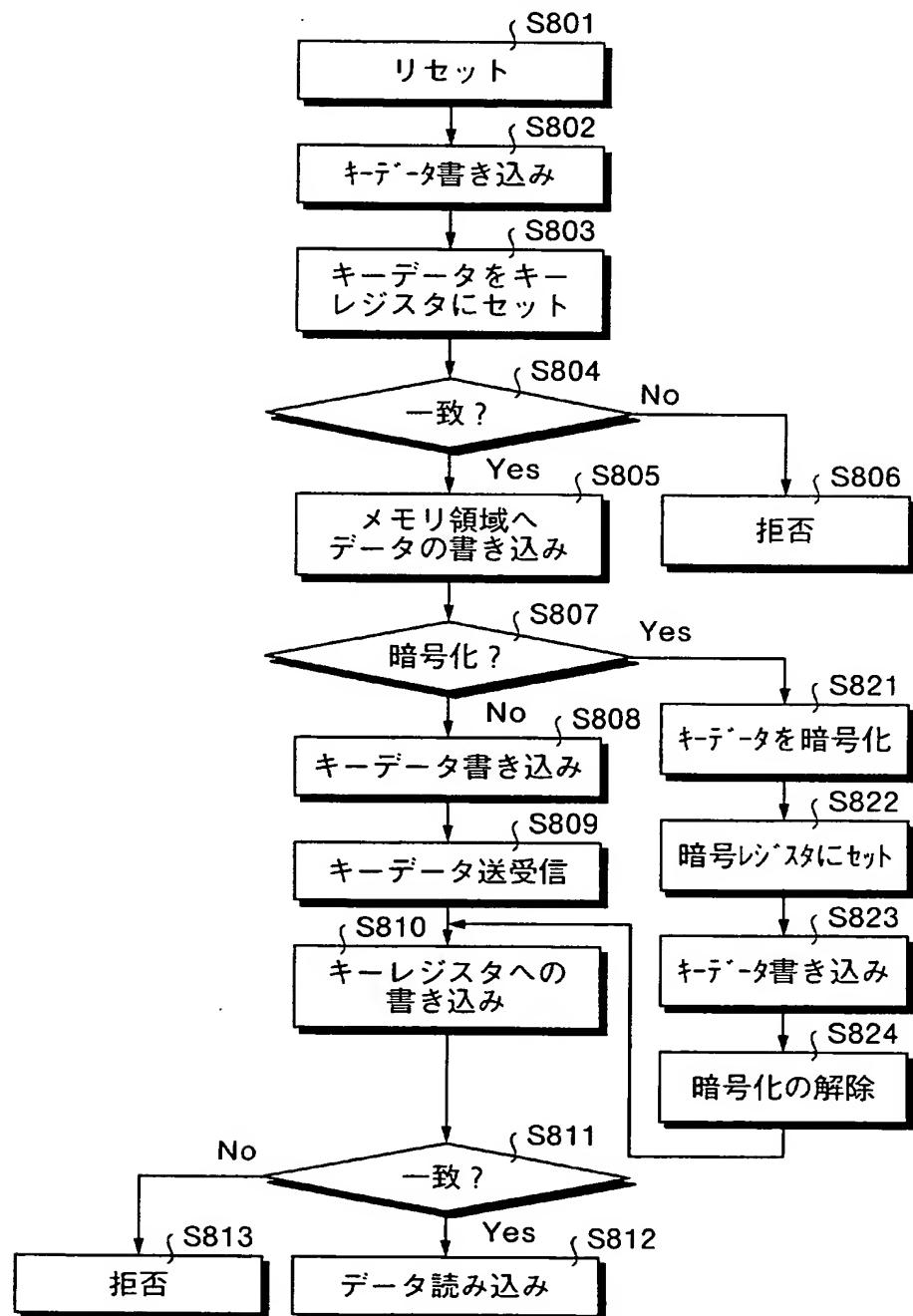
<送り手側>

<受け手側>

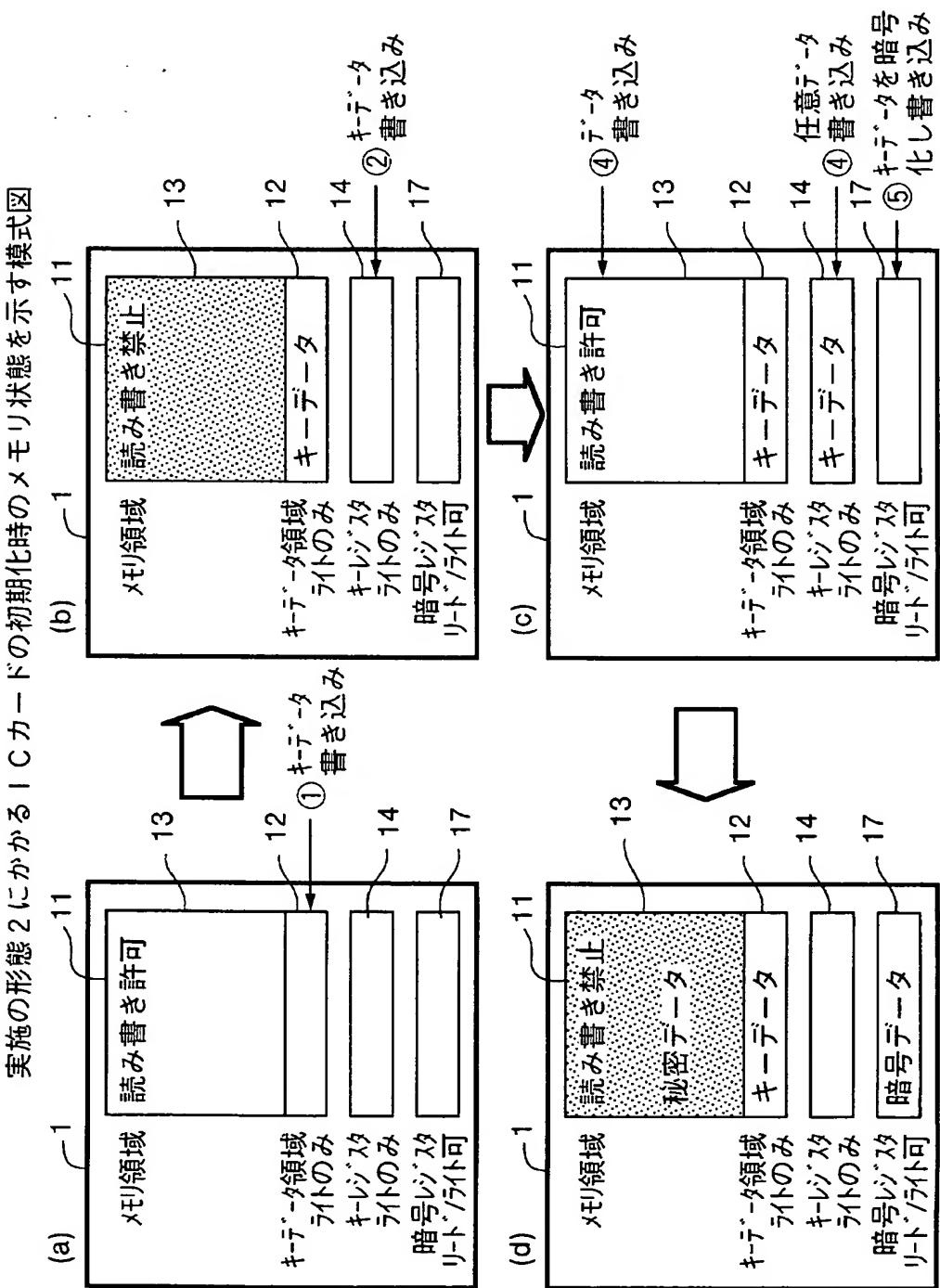


【図 8】

実施の形態 2 にかかる
IC カードへのアクセス方法を説明するフローチャート

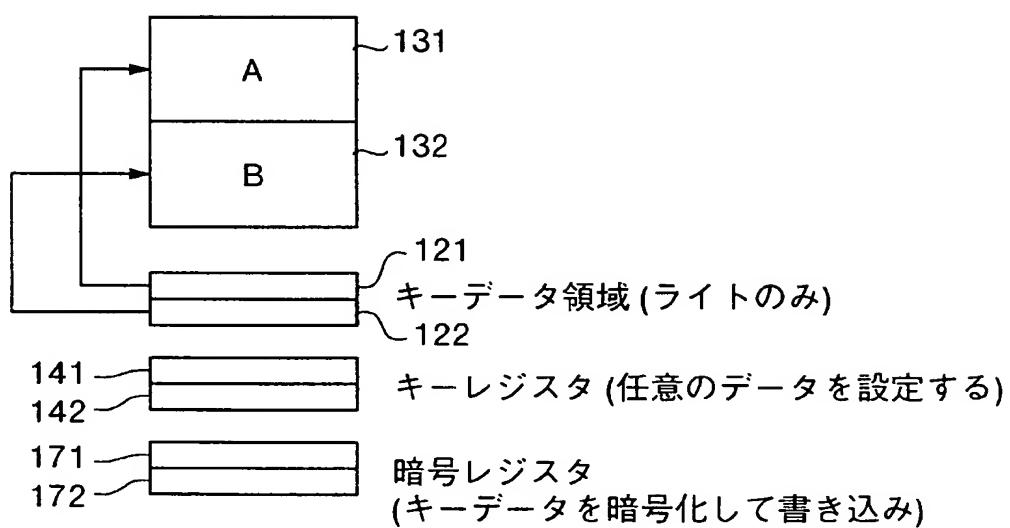


【図9】



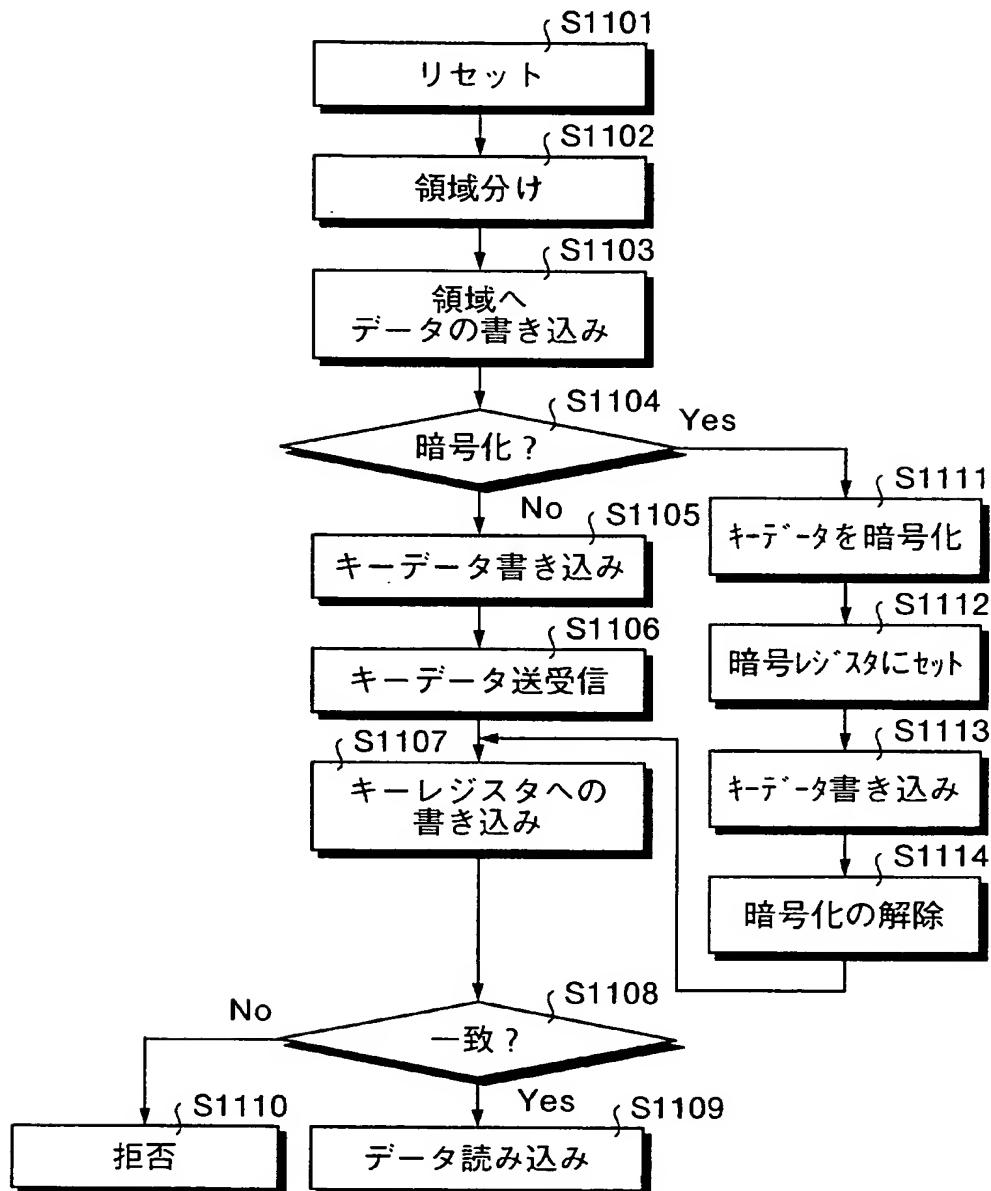
【図10】

実施の形態3にかかるICカードのメモリマップを示す模式図



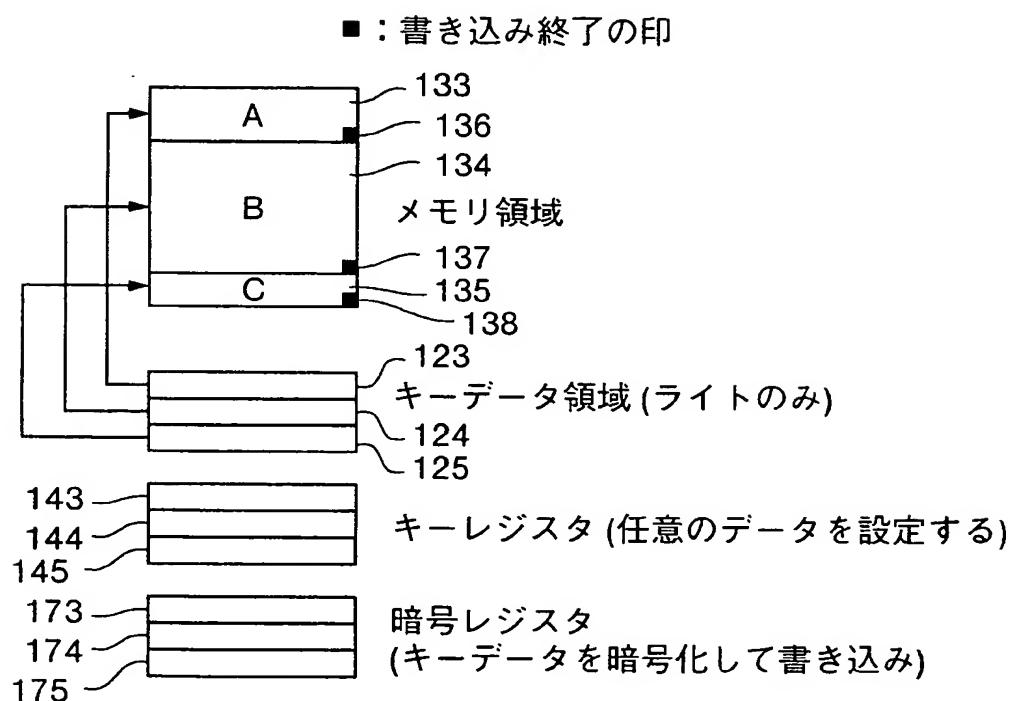
【図11】

実施の形態3にかかる
ICカードへのアクセス方法を説明するフローチャート

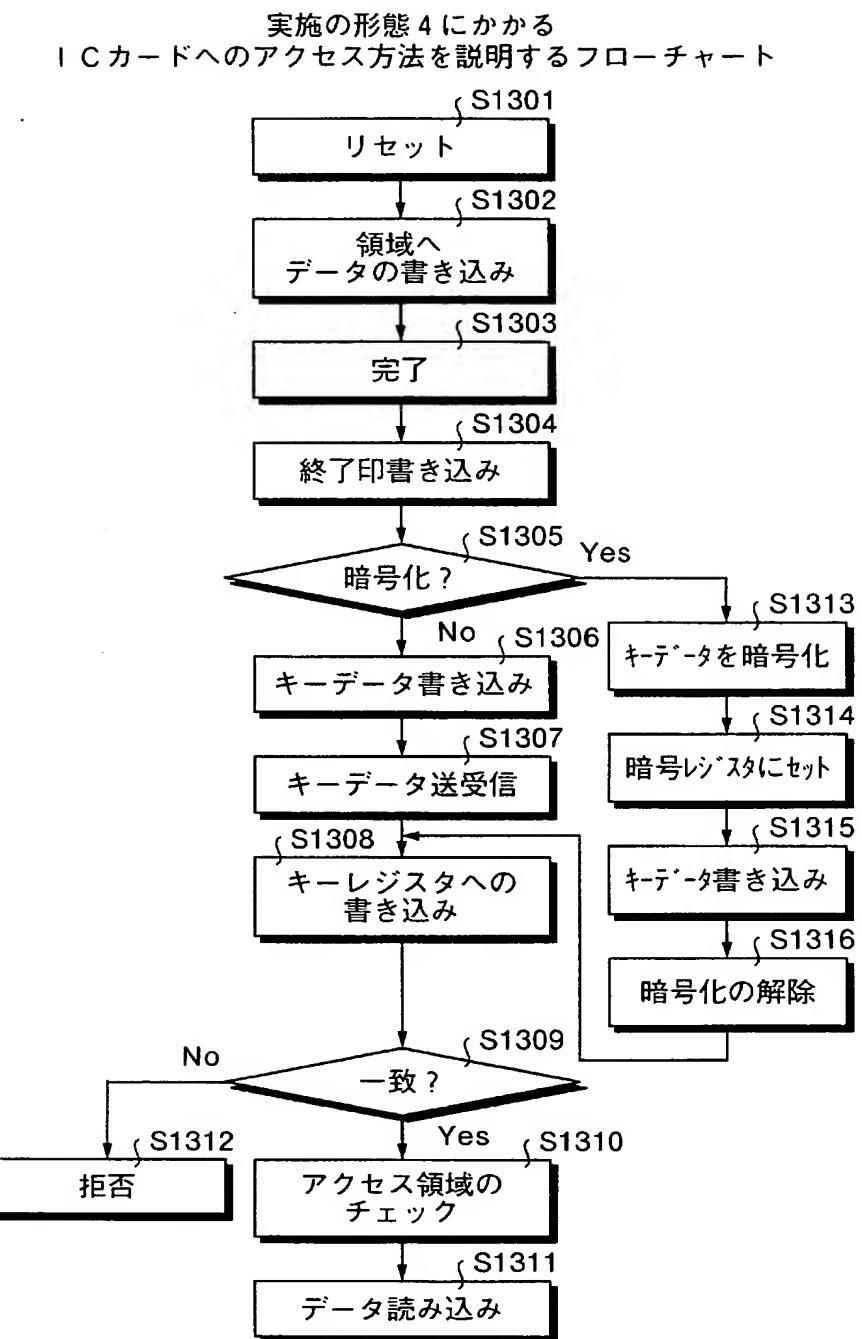


【図12】

実施の形態4にかかるICカードのメモリマップを示す模式図



【図13】



【書類名】 要約書

【要約】

【課題】 ICカードにデータを暗号化することなく記憶させ、その記憶データの漏洩や改ざんを防ぐこと。

【解決手段】 ICカード1に、データの読み出しおよび書き込みが可能な不揮発性のデータ領域13と、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性のキーデータ領域12と、データの書き込みが可能で、かつデータの読み出しが不可能な不揮発性のキーレジスタ14を設ける。データ領域13に暗号化されていない秘密にすべき所定のデータを書き込み、キーデータ領域12にキーデータを書き込むことによって、データ領域13に対するデータの読み出しおよび書き込みを禁止する。データ領域13に対するデータの読み出しまでは書き込みを、キーレジスタ14に正しいキーデータが書き込まれたときに許可し、間違ったキーデータが書き込まれたときに禁止する。

【選択図】 図1

特願2003-097401

出願人履歴情報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日
[変更理由] 住所変更
住所 神奈川県川崎市中原区上小田中4丁目1番1号
氏名 富士通株式会社

特願2003-097401

出願人履歴情報

識別番号 [000237156]

1. 変更年月日 1998年 4月 3日
[変更理由] 名称変更
住 所 東京都日野市富士町1番地
氏 名 株式会社エフ・エフ・シー